DEPARTMENT OF THE AIR FORCE
HQ AIR INTELLIGENCE AGENCY

AIR INTELLIGENCE AGENCY INSTRUCTION 33-106

15 SEPTEMBER 1997

Communications and Information

AIR INTELLIGENCE AGENCY CONFIGURATION MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AIA WWW site at: http://pdo.pdc.aia.af.mil/pubs.

OPR: HQ AIA/DOOI
(Mr. Daniel A. Warniment)

Certified by: HQ AIA/ADO
(Colonel Frank B. Richardson, Jr.)
Pages: 17
Distribution: F; X: AUL/LSE (1); TSS/ADW (2); HQ AIA/DOOI (25)

This instruction implements AFPD 33-1, *Command, Control, Communications and Computer (C4) Systems,* and AFI 33-108, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Computer (C4) Systems.* Air Intelligence Agency (AIA) organizations will use Department of Defense (DoD) Directive 5000.1, Defense Acquisition, DoD Regulation 5000.2-R, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs,* and the Air Force configuration management (CM) methodology to ensure economical and effective life-cycle management of command, control, communications, computer, and intelligence (C4I) systems. This instruction prescribes AIA procedures and guidance for implementing and integrating the CM process for all C4I systems, including automated information systems, for life-cycle sustainment. It also addresses C4 systems requirements which arise from a deficiency in an existing operational capability, from a need for a new capability, or from an opportunity to replace or modernize an existing system with improved technology when operationally and economically practical. This instruction applies to AIA's centers, groups, and wing; it also applies to AIA-gained Air National Guard and Air Force Reserve units. AIA units may supplement this instruction to subordinate organizations. Forward copies of unit supplements to HQ AIA/DOOI, 102 Hall Blvd, STE 227, San Antonio TX 78243-7029.

1. General Information. "Configuration management is a management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life" (Electronic Industries Association Interim Standard National Consensus Standard for Configuration Management).

1.1. CM Process. The CM process provides an organization the means to implement technical and administrative policy direction and adherence, through reviews, to:

1.1.1. Identify, define, and document configuration items and baselines.

1.1.2. Track and control changes to configuration items and baselines.

1.1.3. Record and report change processing and implementation status.

1.1.4. Audit the configuration item and its configuration identification.

1.2. Configuration Management Over the Life Cycle. CM, applied over the life cycle of a product (hardware and software), provides visibility and control of its performance and functional and physical attributes. CM verifies that a product performs as intended and is identified and documented in sufficient detail to support its projected life cycle. Implement CM procedures and guidance in such a way as to complement other AIA processes already established such as the planning and financial processes; systems integration management (SIM); and operational, systems, and technical architecture developments. AIA organizations apply DoD and Air Force CM methodology for all changes to assigned, automated data processing equipment (information technology equipment) and mission equipment, including those systems for which acquisition and CM responsibilities lie with external agencies, such as Air Force Materiel Command (AFMC) organizations or national agencies.

2. Configuration Management Plan (CMP). AIA organizations generate CMPs to define the CM functions as they apply to all systems, system segments, configuration items, and hardware and software developer activities. Document in the CMPs, the systems and equipment which fall under CM and the responsible organizations (include external functional areas such as those within AFMC or national agencies). Information to guide organizations in developing their CMPs is provided in attachment 2. All AIA organizations tailor their CM planning methodology to fit their individual operational, maintenance, and system developmental needs. CM helps program and project management and life-cycle support elements to cope with changes due to evolving missions and technologies. Apply CM in a manner consistent with the complexity, size, quantity, and intended use of systems.

3. Configuration Management Functions. The CM process requires organizations to control their baselines. CM controls the baseline as established by customer needs and program management, not the inventory (that is, all inventory items are not necessarily part of the baselines). AIA organizations document the CM C4I baselines, as identified below, in their individual CMPs.

3.1. Configuration Identification. The configuration identification activity identifies baselines and configuration items (CI) to be brought under CM. Organizations may use the system structure example provided in attachment 3, as a guide to determine the entity to be placed under CM. Establish a CI for all elements of a system (including mission and mission support hardware, software, firmware, communications, interfaces, networks, and documentation). The CI remains applicable throughout all phases of the system's life cycle. The identification is the basic form of which the configuration of products are defined and verified; products and documents are labeled; changes are managed; and accountability is maintained. In support of the identification, define one operational and three standard baselines in the CMP.

3.1.1. Baselines:

3.1.1.1. Functional Baseline (Requirements). Establish the functional baseline to document the approved requirements specifications for each CI. These specification documents translate into operational requirements and the functional characteristics of the system that satisfies the operational need.

3.1.1.2. Allocated Baseline (Design). Establish the allocated baseline by specifying the detailed functional elements sufficiently to begin the detail design process. These documents may be called the system and, or, subsystem specification and the interface control document (ICD).

3.1.1.3. Product Baseline (As-Built). The product baseline is the description of the "as-built" equipment and, or, system in terms of its function, performance, and operational characteristics. The product baseline is established when the necessary "build to" or form, fit, and function requirements for the CI are verified by successful completion of the Functional Configuration Audit (FCA), Physical Configuration Audit (PCA), and the acceptance testing for these requirements.

3.1.1.4. Operational Baseline (As-Installed). Some functional areas may choose to establish an optional fourth baseline. Establish an operational baseline for each CI upon completion of the installation and validation. It is based on the product baseline as updated to accommodate modifications effected during installation, integration, and testing, and reflects the special configuration at a given site.

3.1.2. Identifications:

3.1.2.1. Software Identification. The CMP identifies the naming and version numbering schema for all developmental and commercial off-the-shelf (COTS) software.

3.1.2.2. Hardware Identification. The CMP identifies the numbering schema for each hardware item down to the lowest replaceable unit (LRU) or end item as determined by each organization.

3.1.2.3. Media Identification. The CMP identifies the labeling schema and process for handling all types of media for a specific program, project, or baseline configuration.

3.1.2.4. Documentation Identification. The CMP identifies the numbering schema for all program and, or, project documentation. Configuration documentation defines the functional, performance, and physical attributes of a product and its operational information.

3.2. Change Control. Configuration control is the systematic process of maintaining the formally established baseline identification and regulating all changes to the baseline. Configuration control is achieved through an ordered process of proposal, evaluation, approval or disapproval, and implementation of approved changes to a CI, after a configuration baseline has been established. Configuration control maintains the integrity and continuity of the design, engineering, and cost trade-off decisions which are recorded, communicated, and controlled. Configuration control prevents unauthorized, unnecessary, or marginal changes, while expediting the approval and implementation of those that offer significant benefits. Hardware configuration control for AIA mission systems is managed under DoD 5000.2-R, NSA Circular 80-14, and respective Director, Logistics (AIA/LG) guidance. Document the detailed process for implementing change control in each AIA organization's CMP.

3.2.1. AIA Configuration Steering Group (CSG). The CSG is chartered to ensure compatibility of AIA products with external systems. The charter and the AIA CMP detail membership of this group and its authority. Guidelines are provided for different types of control authorities in attachment 1; each organization's CMP documents the types of control needed and the specific applicable control groups or persons.

3.2.2. Configuration Management Library. CM libraries provide secure, centralized storage areas for project-related documents such as engineering drawings, magnetic media, and software. AIA organizations set up and maintain CM libraries (physical libraries and electronic libraries) according to respective CMPs. Protect physical media from physical damage, contamination, and extremes in temperature and humidity. AIA organizations include in the CMPs a process to cover the archival of original technical data used as the basis for each managed CI, as designated by each organization.

3.3. Configuration Status Accounting. AIA organizations use and manage CM reports which meet their CM needs. CM reports provide the information necessary to trace and maintain status of configuration items, baselines, and other related items within the configuration management process. These reports provide a record of decisions made, promulgated, and follow-up or verification of decision implementation. They also provide a snapshot of the product at any time and identify all related supporting technical data. Organizations document their report process in the CMPs.

3.4. Configuration Audits and Reviews. Perform configuration audits to verify, validate, and document the CI. Configuration audits ensure the appropriate specifications and other support documents are in agreement, are accurate and complete, and have satisfied the total program requirements. Wherever practicable and appropriate, configuration audits are accomplished in conjunction with other audits, reviews , demonstrations, inspections, or test and evaluation activities. Requirements for these audits and reviews are normally specified in the CMP, but they can be specified in the program, project, or quality plans as appropriate. Program or project managers are responsible for ensuring that configuration audits are performed.

3.4.1. Functional Configuration Audit (FCA). The system project team, as designated by the system Program Manager, with configuration management support, conducts FCAs following the criteria specified in the requirements documentation or the statement of work, if available. (The Statement of Work is used instead of a functional or an allocated baseline.) If the product does not perform in compliance with requirements and specifications, take the corrective actions defined in the CMP.

3.4.2. Physical Configuration Audit (PCA). During the PCA the responsible office traces the product through its baselines, verifies its physical characteristics (form and fit) as described in supporting documents (for example, manuals and drawings), and conducts a final review of all supporting documentation to ensure that traceability exists through the product's life cycle. The result of the PCA is a formal acknowledgment that the product matches the physical description in its documentation and ensures that the product meets the customer needs.

3.4.3. Other Audits. Depending on the size and complexity of the system under control, other audits may be conducted to help ensure complete traceability of the requirement throughout the life cycle. The AIA Inspector General (AIA/IG) office may inspect to ensure compliance to AIA CM policy. AIA may request an audit be performed at any time throughout the life of a system or software application.

4. Other Functional Organizations. Organizations may try to meet CM requirements with existing management and board structures. Organizations should make best use of efficient technical and managerial tools which already work. Organizations include in their CMPs the relationships with other functional groups. As a minimum, the CMP includes the relationships of program and project managers, the

Systems Integration Management Office (SIMO), and the Information System Security Officer (ISSO). Set up new CM activities only when absolutely essential to meet the intent of CM policy.

4.1. Project and Program Management. The project and program management organizations are crucial to ensuring that every office affected by a change to the existing baselines are aware of the change and can react to the change when it is scheduled. Proper scheduling and interfacing between different components of the organization minimize impacts on personnel resources and the completion of the project.

4.2. Systems Integration Management Office (SIMO). The SIMO representatives from organizations review changes to the baselines to determine whether they meet DoD standards. A key SIMO role is maintaining the logical-level baseline required by the Air Force and national-level SIMO functions. The SIMO complies with technical matters of the system perspective according to DoD standards and guidelines. The SIMO maintains an interactive role in meetings and, or, seminars to ensure the flow of communication and understanding so that organizations can properly implement standards as well as relay the requirements and, or, impacts to the involved AIA organizations.

4.3. Data Administrator (DAd). The data administrator ensures that data used to support system development is managed according to DoD standards and guidelines. Baseline changes and modifications resulting from software upgrades should incorporate standard data elements to alleviate the possibility of redundancy or inconsistency across Air Force systems and to ensure that data is managed accordingly as a shared corporate resource.

4.4. Information System Security Officer (ISSO). The ISSO representatives ensure that all appropriate security directives are followed in changing the baselines. The ISSO ensures that systems conform to security requirements and does not allow changes to be added to a system that might corrupt its integrity. One role of the ISSO is to review the proposed projects and to ensure that resources are not wasted by acquiring infrastructure components unable to be fully used due to security constraints.

5. References. Documents containing DoD and Air Force direction and guidance about CM are listed in attachment 1. The Electronic Industries Association (EIA) Interim Standard National Consensus Standard for CM is expected to become basic guidance in DoD and Air Force CM direction.

G. THOMAS BAKER, Colonel, USAF
Assistant Director of Information Operations

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS AND ACRONYMS, AND TERMS

References

AFI 33-108, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Computer (C4) Systems,* 14 Jul 94.

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems,* 19 Sep 93.

Department of Defense Intelligence Information System (DODIIS) Configuration Management Plan, 22 Apr 93.

DoD Directive 5000.1, *Defense Acquisition,* 15 Mar 96.

DoD Regulation 5000.2-R, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs,* 15 Mar 96.

EIA/IS-649, *Electronic Industries Association (EIA) Interim Standard National Consensus Standard for Configuration Management,* Aug 95.

JDODIIS, *Joint DODIIS/Cryptologic SCI Information Systems Security Standards,* 28 Mar 97.

Military-Standard-973, *Configuration Management,* 17 Apr 92, with latest Notice Change 3, 13 Jan 95.

NSA/CSS Regulation No. 80-14, *National Security Agency/Central Security Service, Configuration Management,* 19 Sep 95.

NSA/CSS Cir. No 80-18, *National Security Agency/Central Security Service, Modification Work Orders/ Software Upgrade Description Documents,* 19 Sep 95.

NSA-CM-HDBK, National Security Agency Configuration Management Implementation Guide, 15 Sep 93.

Abbreviations and Acronyms

ADPE—Automated Data Processing Equipment

AFPD—Air Force Policy Directive

AIA—Air Intelligence Agency

C4—Command, Control, Communications, and Computer

C4I—Command, Control, Communications, Computer, and Intelligence

CCB—Configuration Control Board

CI—Configuration Item

CM—Configuration Management

CMP—Configuration Management Plan

CMWG—Configuration Management Working Group

COTS—Commercial off-the-shelf

CSAR—Configuration Status Accounting Report

CSG—Configuration Steering Group

CSU—Computer Software Unit

DoD—Department of Defense

DODIIS—Department of Defense Intelligence Information System

EIA—Electronic Industries Association

ERB—Engineering Review Board

FCA—Functional Configuration Audit

F/W—Firmware

HCCB—Hardware Configuration Control Board

HWCI—Hardware Configuration Item

ICD—Interface Control Document

ICWG—Interface Control Working Group

IG—Inspector General

IPMS—PC-based Information Processing Management System

ISSO—Information System Security Officer

LRU—Lowest Replaceable Unit

NSA/CSS—National Security Agency/Central Security Service

PCA—Physical Configuration Audit

PET—Position Equipment Tables

SCCB—Software Configuration Control Board

SIM—Systems Integration Management

SIMO—Systems Integration Management Office

SWCI—Software Configuration Item

TIM—Technical Interchange Meeting

Terms

Acceptance—The process by which the customer's representative formally agrees to ownership of a completed product.

Accreditation—The official command authorization to operate an automated information system or network and is based in part on the formal certification of the system to meet a prescribed set of security requirements.

Baseline—A configuration identification document or set of documents formally designated and fixed at a specific time during a Configuration Item's life cycle. Baselines, plus approved changes from those

baselines constitute a system's configuration identification. Throughout the life cycle of a program or project, CM establishes three control baselines: allocated, functional, and product.

Baseline Management—The application of technical and administrative direction to designate and control configuration identification at discrete points in the life cycle.

C4I System—Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control, through all phases of the operational continuum. This includes base visual information support systems.

Communications Media—A medium or means for transferring analog or digitized formatted data. Includes modems, multiplexers, cryptologic equipment, line drivers, cable protocols, protocol handlers, data rates, and modes of transmission.

Computer Hardware—Devices capable of accepting and storing computer data, executing a systematic sequence of operations on computer data, or producing control outputs.

Computer Software—A combination of computer instructions and computer data definitions that enable the computer to perform computational or control functions. Software categories are mission operational, mission support, system operational, and system support.

Configuration—The complete technical description required to build, test accept, operate, maintain, and logistically support equipment. Also includes the physical and functional characteristics of the equipment.

Configuration Item (CI)—A collection of hardware or software, or any of its parts, that satisfies an end use and is designated by the government or customer for configuration management.

Corollary Change—A change required as a direct result of some other change. For example, a change to a circuit board in a Digital Equipment Corporation computer may require a simultaneous change in a similar circuit board at a SUN SPARC computer in order to insure a consistent reliable interface between the two systems.

Deviation—The written customer acceptance document for an item that does not meet a specific contractual requirement.

Electronic Library—A secure CM electronic program library set up within the development environment of a configuration-managed project for the control and release of deliverable versions of software. The program library may contain any or all of the following three major types of library: Project Support Library (software development working library; Master Library (latest baselined software and document for the CI); Archive Library (archive items for previous versions).

Firmware (F/W)—The combination of a hardware device and computer instructions or computer data that resides as read-only software on the hardware device. The software cannot be readily modified under program control. This definition also applies to read-only digital data that may by used by electronic devices other than digital computers.

Form, Fit, and Function—The physical and functional characteristics of a CI as an entity, but not covering characteristics of the elements making up the CI.

Functional Configuration Audit—A formal examination of the test data on functional characteristics for a configuration item, prior to acceptance, to verify that the item has achieved the performance

specified in its functional or allocated configuration identification. The FCA validates that development and implementation of a system is complete.

Integrated Logistics Support—A grouping of elements for assuring effective and economical support of equipment at all maintenance levels for its planned life cycle. These elements include: facilities, maintenance, support equipment, logistics data, spares and repair parts, logistics support personnel, and contract maintenance.

Physical Configuration Audit—A formal audit to verify that an "as-built" configuration item conforms to the defining technical documentation. The PCA validates the form and fit of the product and ensures that the product meets the customer needs.

Physical Library—The CM physical library provides a central repository for all reports, forms, documents, drawings, and computer listings for configuration items. Secure storage (for example, drawers and file cabinets) will be provided for documentation and drawing masters, magnetic media, and firmware. The media used for computer program storage include removable hard disks and floppy disks.

Quality Assurance—The system, procedures, and activities for assuring that an item will perform satisfactorily in actual operation by verifying that materials, construction, and testing meet the requirements of project and procurement specifications.

System—A grouping of subassemblies, assemblies, and equipment that provides a specific function. A system may also include personnel and facilities**.**

CM Boards and Groups—NOTE: Many different types of control boards and groups can be implemented at each organization. The key is to define the type of board, group, or review structure the individual AIA organization finds best for its needs. This is documented in the individual CMPs. Organizations use whatever board, group, or review processes are currently in place and working, and document those processes. The following are examples and short descriptions of different types of boards or groups that may be used; other types of boards and groups can be generated based upon the type of control needed.

Configuration Steering Group (CSG)—The AIA CSG, whose composition and purpose will be established by charter, enacts AIA policy on CM. The role of this steering group is to ensure that organizational communications and computer changes meet the CM guidelines established in AIA's CMP.

Configuration Control Board (CCB)—The CCB is a board composed of technical and administrative representatives who recommend approval or disapproval of proposed changes to a baseline, recommend approval or disapproval of proposed deviations from currently approved configuration baseline, and direct and ensure implementation of approved changes. The group also ensures documentation updates are completed as required.

Software Configuration Control Board (SCCB)—A committee established to review proposed software changes and to direct planning and implementation of approved changes.

Hardware Configuration Control Board (HCCB)—A group established to review and control all changes to the hardware and peripherals of a set configuration or baselines.

Engineering Review Board (ERB)—An ERB is established to provide advice and consultant support to the CCB on technical matters. The ERB is responsible for providing cost, benefits, technical, and risk assessment analyses for proposed changes and additions to baseline products, standards, and documents;

for validating the findings of Integration Test Facilities; and for staying abreast of emerging technology**.**

Interface Control Working Group (ICWG)—An ICWG is established by direction from the CCB to provide technical and administrative coordination of interfaces. ICWGs are expected to be required for common interfaces among products, key projects, and legacy systems. ICWGs may also be established for products that have an interface with common commercial products to minimize the development of unique solutions for such interfaces and changes to the interfaces when promulgated by the commercial product.

Technical Interchange Meeting (TIM)—The Technical Interchange Meeting (TIM) brings together a group, consisting of the customer, the program manager, and appropriate individuals from the technical implementation organizations to determine if new proposed requirements should go to the CCB for approval; determine if proposed changes are valid and require a material solution; and to conduct a forum to discuss system problems or new capabilities.

Configuration Management Working Group (CMWG)—The CMWG is a working group, composed of the user and implementing agencies to provide the status of approved changes to the system, resolve issues, and keep CCB members informed on all aspects of the configuration control process.

Functional Level Group or Position—Functional level group or position is the organizational element that is responsible for supporting a segment of AIA's C4I support. Following implementation of the configuration plan, these groups or positions are responsible for maintaining CM guidelines and for coordinating with the CCB all proposed changes to the AIA computing infrastructure.

Attachment 2

CONFIGURATION MANAGEMENT PLAN INFORMATION CONFIGURATION MANAGEMENT PLAN OUTLINE

A2.1. Each Air Intelligence Agency organization shall develop and document its configuration management (CM) guidelines and plans. Performing CM planning for the product and its environment is essential. Because it clearly and concisely describes the process, a well documented configuration management plan (CMP) is useful both for training of personnel and for explaining the process to customers, quality assessors, and auditors. If an organization has an operations plan or series of other documents which implement CM needs, these documents may be sufficient to fill the CMP requirements. Figure A2.1 is a representative format and description of content of a CMP which can be tailored to meet each organization's individual program and project planning needs.

Figure A2.1. Format and Description of Contents.

1. Introduction

1.1. Purpose

1.2. Scope

1.3. Terms and Acronyms

1.4. References

2. Management Overview

2.1. Organization

2.2. Responsibilities

2.3. Programmatic and organizational Interface Management

2.4. Implementation

2.5. Integration of Configuration Management

2.6. Applicable Practices and Procedures

3. Configuration Management Activities

3.1. Configuration Identification

3.2. Configuration Control

3.3. Configuration Status Accounting

3.4. Configuration Audits/Reviews

3.5. Configuration Management of digital data

4. Methods, Techniques, and Tools

5. Deliverables, milestones, and schedules

6. Contractor/Subcontractor and Supplier Control (if applicable)

7. Record Collection and Retention

A2.2. Description of Sections: The following table provides representative format and content of each of the sections listed in the outline of a CMP. This outline is flexible enough to allow organizations to tailor to their needs in order to plan a workable CM solution. The asterisk (*****) preceding sections below indicates information which should be part of each CMP.

Table A2.1. Description for Sections.

Section	Title	Description
1.	Introduction	
*1.1	Purpose	Define the purpose of the CMP.
*1.2	Scope	Define items maintained under configuration control as well as the organization, activities, and phases of the life cycle to which the plan applies.
1.3	Terms and Acronyms	Define or provide a reference to definitions of all terms and acronyms required to properly interpret the CMP.
1.4	References	Provide a complete list of documents referenced elsewhere in the CMP. Specify sources from which the referenced documents can be obtained.
*2.	Management Overview	
2.1	Organization	Describe the organizational structure of the CM program. Specifically define: CM team; CM reporting structure; CCB and working groups, as required.
*2.2	Responsibilities	Define responsibilities for identification, control, status accounting, reviews, and audits. Define the responsibilities of the CCB and other sub-boards, as needed.
2.3	Programmatic and Organizational Interface Management	Define the approach to: defining interfaces to the external environment; and controlling changes to the interfaces.
*2.4	Implementation	Define the major milestones for implementation of the CMP. Examples of milestones include: review of the CCB membership; each applicable configuration baseline and release; and schedules for CM reviews and audits.
2.5	Integration of Configuration Management	Define the usage of all CM tools. Explain how the CM system coexists with other development tools, fully integrated into the life-cycle process.

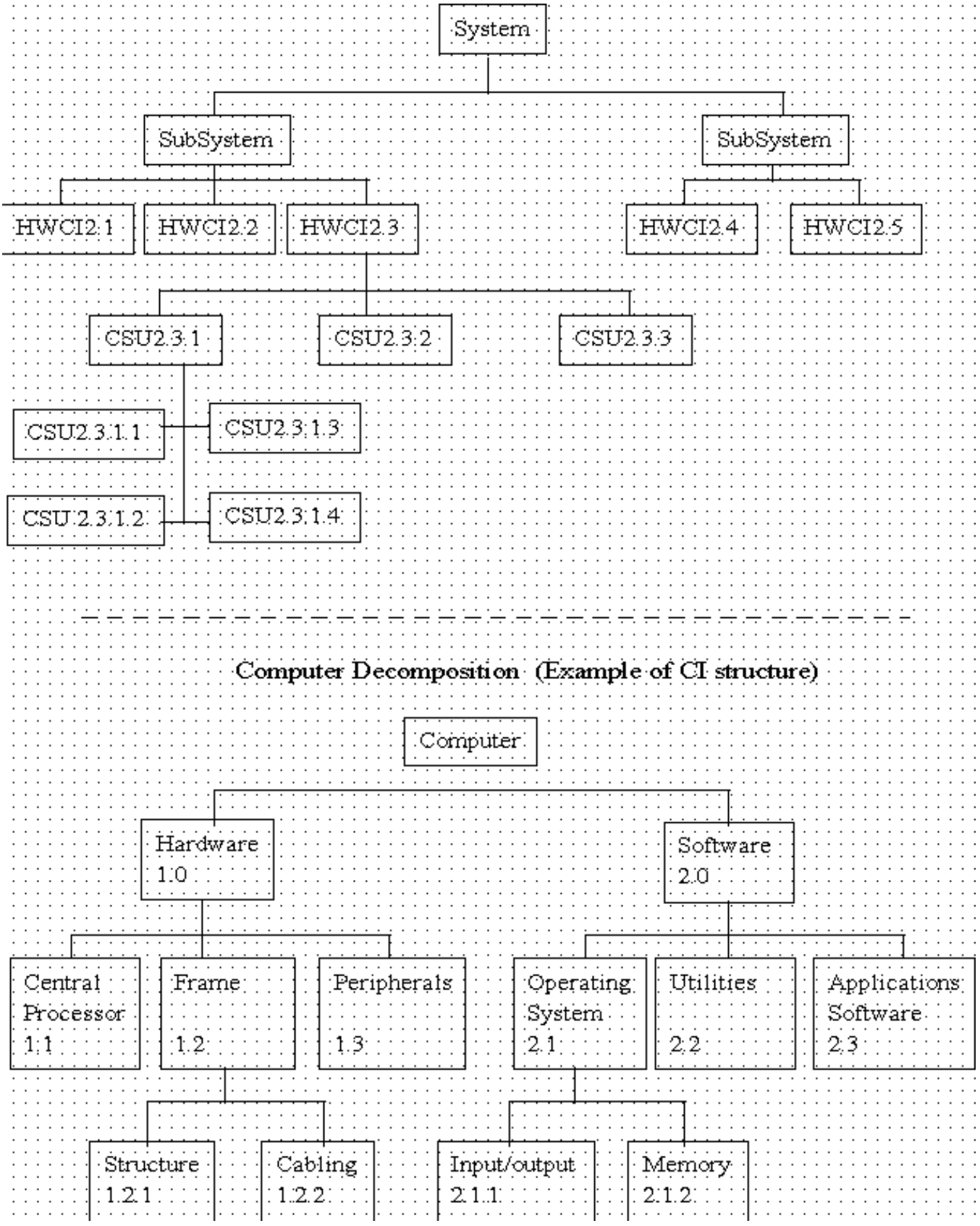
2.6	Applicable Practices and Procedures	Define all applicable CM polices, directives, and procedures implemented as part of this plan. Define CM procedures. Examples include: naming conventions; version-level designations; configuration identification approach; document release process; change order processing; library system operations; auditing process; funding and approval procedures; engineering change order release and tracking; and acceptance and signoff procedures.
3.	Configuration Management Activities	
3.1	Configuration Identification	Define the solution baselines and correlate them to the specific life-cycle phases. For each baseline, describe the following: the items that form the baseline; the review and approval events; and the acceptance criteria associated with the establishment of each baseline. Detail procedures for the titling, labeling, numbering, and cataloging of all CIs.
3.2	Configuration Control	Define methods to be used to process change orders, including: the procedure for implementing approved change orders; procedures for library control, such as access control, archive maintenance, change history, and disaster recovery. Define procedures to be used for configuration of interfaces with programs or projects beyond the scope of this CMP. State control procedures for associated items (for example, for standard products or customer-developed systems).
3.3	Configuration Status Accounting	Define how information on the status of CIs is collected, verified, stored, processed, and reported. Identify the periodic reports and how they are distributed. State dynamic inquiry capabilities provided. Describe the means of implementing any special status accounting requirements specified by the customer.
3.4	Configuration Audits and, or, Reviews	Define the CM role in audits and reviews performed at specified points in the life cycle. Identify the CIs covered at each audit and review. State the procedures used for identifying and resolving problems that occur during these audits and reviews.
3.5	CM of Digital Data	
4.	Methods, Techniques, and Tools	Define the methods, techniques, and tools that will be employed to support CM of the program or project.
5.	Deliverables, Milestones, and Schedules	List all the deliverables and standards/data item descriptions. List all milestones and schedules, to include any pert charts, spreadsheets, or graphics.

6.	Contractor and, or, Subcontractor and Supplier Control	Describe provisions for ensuring that contractor and, or, subcontractor-provided and supplier-provided solution components meet established CM requirements. At a minimum, contractors and, or, subcontractors and suppliers are required to prepare and implement their own CMP in accordance with the one described here.
7.	Record Collection and Retention	Identify the CM documentation retained. State the methods and facilities that will be used to safeguard and maintain this documentation (for example, identify any off-site facilities used). Designate the retention period.

Attachment 3

SYSTEM STRUCTURE

Figure A3.1. System Structure and Computer Decomposition (Example of CI Structure).



CSU - Computer Software UnitHWCI - Hardware Configuration Item